WHAT IS CLAIMED IS:

1. A network gateway device comprising:

a network physical interface for receiving and transmitting data and for receiving packets for transmission and forwarding packets from received data; and

a packet processor hosting a security association (SA) used for encryption and decryption for communication with a network peer and including:

an ingress processing security subsystem with a decryption processor for decrypting packets; and

an egress processing security subsystem for encrypting packets, one or both of said ingress processing security subsystem and said egress processing security subsystem receiving one or both of ingress and egress SAs.

2. A network gateway device according to claim 1, wherein said packet processor includes a processor subsystem for handling key exchanges and for distributing SAs to the ingress processing security subsystem and said egress processing security subsystem.

3. A network gateway device according to claim 1, wherein said ingress processing security subsystem and said egress processing security subsystem hosts

a security association (SA) used for encryption and decryption for communication with a network peer and one of said ingress processing security subsystem and said egress processing security subsystem distributing at least one of ingress and egress SAs to the other of said ingress processing security subsystem and said egress processing security subsystem.

4. A network gateway device according to claim 1, wherein said packet processor includes an ingress processor system for ingress processing of received packets and an egress processor system for processing packets for transmission, said ingress processor system including an ingress packet processor and including said ingress processing security subsystem, said egress processor system including an egress packet processor and including said egress processing security subsystem and interconnections including an interconnection between said ingress processor and said egress processor, an interconnection between said ingress processor and said physical interface and an interconnection between said ingress processor and said physical interface.

5. A network gateway device according to claim 4, wherein said ingress processing security subsystem includes memory and a hardware accelerator for running decryption algorithms, said ingress processing security subsystem includes memory and a hardware accelerator for running decryption algorithms.

6. A network gateway device according to claim 4, further comprising a packet queue establishing a queue of packets awaiting transmission, said packet queue being the exclusive buffer for packets between packets entering the device and packet transmission.

7. A network gateway device according to claim 6, wherein packets exit the device at a rate of the line established at the physical interface.

8. A network gateway device according to claim 4, wherein said ingress processing system processes packets including at least one or more of protocol translation, de-encapsulation, decryption, authentication, point-to-point protocol (PPP) termination and network address translation (NAT) and said egress processing system processes packets including at least one or more of protocol translation, encapsulation, encryption, generation of authentication data, PPP generation and NAT.

9. A network gateway device according to claim 4, wherein said ingress processor system includes a fast path processor subsystem processing packets at speeds greater than or equal to the rate at which they enter the device.

10. A network gateway device according to claim 9, wherein said fast path processor system provides protocol translation processing converting packets from

one protocol to another protocol.

11. A network gateway device according to claim 9, wherein said egress processor system includes a fast path processor subsystem processing packets at speeds greater than or equal to the rate at which they are to leave the device.

12. A network device according to claim 9, wherein said ingress processor system includes a fast path co-processor for additional packet processing concurrently with fast path processor packet processing, said fast path co-processor processing packets including one or more of network address translation (NAT) processing and NAT processing coupled with application layer processing (NAT-ALG).

13. A network device according to claim 9, wherein said ingress processor system includes a control packet processor for additional packet processing concurrently with fast path processor packet processing, including processing packets signaling the start and end of data sessions, packets used to convey information to a particular protocol and packets dependent on interaction with external entities.

14. A network device according to claim 4, wherein said physical interface includes a line card and said ingress processor system is provided as part of a service card and said egress processor system is provided in one of said service card and

another service card and said interconnections include:

a line card bus connected to said line card;

a service card bus connected to at least one of said service card and said another service card; and

a switch fabric connecting said line card to at least one of said service card and said another service card.

15. A network device according to claim 14, wherein said service card includes said ingress processor system and said egress processor system and said another service card includes another ingress processor system for processing all or part of packets received from said line card and for sending ingress processed packets for egress processing and another egress processor system for receiving ingress processed packets and for processing all or part of received packets for sending to said line card, whereby packets may be sent between service cards for ingress processing by one service card and egress processing by another service card or for ingress processing using more than one service card.

16. A network gateway device according to claim 15, wherein each of said service cards is identical and a spare service cards is provided, for functionally replacing any one of the other service cards to provide redundancy.

17. A network gateway device according to claim 15, wherein said physical

interface includes another line card connected by said switch fabric to at least one of said service card and said another service card.

18. A network gateway device according to claim 17, wherein said switch fabric connects any one of said line cards to any one of said service cards, whereby any line card can send packet traffic to any service card and routing of packet traffic is configured one of statically and dynamically by the said line card.

19. A network gateway device according to claim 15, wherein:

said service card bus includes a static bus part for connection of one of said service cards through said switch fabric to one of said line cards and a dynamic bus for connecting a service card to another service card through said fabric card allowing any service card to send packet traffic requiring ingress processing to any other service card for ingress processing and allowing any service card to send traffic requiring egress processing to any other service card for egress processing, whereby the system can make use of unused capacity that may exist on other service cards.

20. A process for secure communication between network entities, the process comprising the steps of:

providing a device with a network interface and physical connection with a packet processing system including an ingress processing subsystem and an egress

processing subsystem;

making a key exchange between the network entity and the other network entity and hosting a security association upon completion of the key exchange in association with a processing entity of the packet processing system, the security association including information as to authentication, encryption and changing of keys;

extracting data derived from the security association;

sending a message from a processing entity hosting the security association to one or both of said ingress processing subsystem and said egress processing subsystem to provide a security association at the processing subsystems.

21. A process according to claim 20, wherein said packet processor includes an ingress processing security subsystem and an egress processing security subsystem and a processor subsystem for handling key exchanges and for distributing SAs to the ingress processing security subsystem and said egress processing security subsystem.

22. A process according to claim 20, wherein said packet processor includes an ingress processing security subsystem and an egress processing security subsystem, one of said ingress processing security subsystem and said egress processing security subsystem hosting the security association used for encryption and decryption for communication with a network peer said one of said ingress

processing security subsystem and said egress processing security subsystem distributing at least one of ingress and egress SAs to the other of said ingress processing security subsystem and said egress processing security subsystem as a security message.

23. A process according to claim 22, further comprising:

selecting either the ingress processing subsystem or the egress processing subsystem to host a security association.

24. A process according to claim 22, wherein said security message includes authentication features for authenticating the transmission of said session data.

25. The process according to claim 22, further comprising the steps of establishing a shared secret key at each of the ingress processor and egress processor for use for symmetric block encryption; and encrypting said session data using the symmetric block encryption cipher.